

Enterprise Vault™

审核

12.3

Enterprise Vault™：审核

上次更新日期： 2018-03-09。

法律声明

Copyright © 2018 Veritas Technologies LLC. © 2018 年 Veritas Technologies LLC 版权所有。All rights reserved. 保留所有权利。

Veritas、Veritas 徽标、Enterprise Vault、Compliance Accelerator 和 Discovery Accelerator 是 Veritas Technologies LLC 或其附属公司在美国和其他国家/地区的商标或注册商标。其他名称可能为其各自所有者的商标，特此声明。

本产品可能包含 Veritas 必须向第三方支付许可费的第三方软件（以下称“第三方案序”）。部分第三方案序会根据开源或免费软件许可证提供。软件随附的授权许可协议不会改变这些开源或免费软件许可证赋予您的任何权利或义务。请参考此 Veritas 产品随附的或以下链接提供的第三方法律声明文档：

<https://www.veritas.com/about/legal/license-agreements>

文档中介绍的产品根据限制其使用、复制、分发和反编译/逆向工程的授权许可协议分发。未经 Veritas Technologies LLC 及其特许人（如果存在）事先书面授权，不得通过任何方式、以任何形式复制本文档的任何部分。

本文档按“现状”提供，对于所有明示或暗示的条款、陈述和保证，包括任何适销性、针对特定用途的适用性 or 无侵害知识产权的暗示保证，均不提供任何担保，除非此类免责声明的范围在法律上视为无效。Veritas Technologies LLC 不对任何与提供、执行或使用本文档相关的伴随或后果性损害负责。本文档所含信息如有更改，恕不另行通知。

根据 FAR 12.212 定义，授权许可的软件和文档被视为“商业计算机软件”，享有适用的 FAR 第 52.227-19 节“Commercial Computer Software - Restricted Rights”（商业计算机软件 - 受限权利）和 DFARS 第 227.7202 节及后续“Commercial Computer Software and Commercial Computer Software Documentation”（商业计算机软件和商业计算机软件文档）中定义的受限权利，而不论 Veritas 是在本地还是以托管服务的形式提供这些软件和文档。美国政府仅可根据本协议的条款对授权许可的软件和文档进行使用、修改、发布复制、执行、显示或披露。

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

<https://www.veritas.com>

技术支持

技术支持具有全球性支持中心。所有支持服务都将按照与您达成的支持协议和当前的企业技术支持策略予以提供。有关我们的支持服务，以及您如何与技术支持部门联系的信息，请访问我们的网站：

<https://www.veritas.com/support>

您可以通过以下 URL 管理您的 Veritas 帐户：

<https://my.veritas.com>

如果您对现有支持协议有任何疑问，请向您所在地区的支持服务协议管理团队发送电子邮件，如下所示：

全球（不包括日本）

CustomerCare@veritas.com

日本

CustomerCare_Japan@veritas.com

在与技术支持联系之前，请运行 Veritas Quick Assist (VQA) 工具，确保符合产品文档中所列的系统要求。可以从 Veritas 技术支持网站上的以下文章中下载 VQA：

https://www.veritas.com/support/en_US/vqa

文档

请确保您具有文档的最新版本。每个文档在第 2 页显示上次更新日期。Veritas 网站上提供了最新文档：

<https://www.veritas.com/docs/100040095>

文档反馈

您的反馈信息对我们很重要。提供文档改进建议，或报告文档的错误或疏漏。请随附您所报告的文档标题、文档版本、章节标题和文本小节标题。请将反馈发送到：

evdocs@veritas.com

您也可在 Veritas 社区站点上查看文档信息或提出问题：

<https://www.veritas.com/community>

目录

第 1 章	关于本指南	5
	指南简介	5
	从何处获取有关 Enterprise Vault 的详细信息	5
	Enterprise Vault 培训模块	7
第 2 章	Enterprise Vault 审核简介	8
	关于 Enterprise Vault 审核功能	8
第 3 章	设置审核	10
	设置审核	10
	创建审核数据库	11
	配置审核类别	12
	启动或停止审核	14
	调整审核	15
	移动审核数据库	15
第 4 章	查看审核数据库条目	17
	关于查看审核数据库条目	17
	使用审核查看器查看审核数据库条目	17
	使用审核查看器运行审核数据报告	17
	从审核查看器中复制搜索结果	19
	更改审核查看器设置	19
	使用 SQL 查询查看审核数据库条目	19
	以用户友好格式检索归档权限的审核更改	20
第 5 章	审核数据保护合规性	22
	审核常规删除操作	22
	常规项目删除审核条目的查询搜索示例	23
	审核特权删除操作	25
	查询搜索特权删除审核条目示例	26
附录 A	审核数据库条目的格式	27
	审核数据库条目的格式	27

关于本指南

本章节包括下列主题：

- [指南简介](#)
- [从何处获取有关 Enterprise Vault 的详细信息](#)

指南简介

本指南介绍如何设置 Enterprise Vault 审核。

Enterprise Vault 的审核功能按许多不同的类别记录活动。选择要记录活动的类别，Enterprise Vault 会将记录的信息存储在 Enterprise Vault 审核数据库中。然后，您可以使用 SQL 查询查看审核数据库条目，或者使用审核查看器实用程序。

审核功能是证明遵从数据保护法规的重要工具。例如，您可以使用 Enterprise Vault 分类来标记个人身份信息 (PII)，然后启用审核以记录删除 PII 的时间。

从何处获取有关 Enterprise Vault 的详细信息

[表 1-1](#) 列出了 Enterprise Vault 附带的文档。Veritas [文档库](#)中还提供了 PDF 和 HTML 格式的此文档。

表 1-1 Enterprise Vault 文档集

文档	注释
Veritas Enterprise Vault 文档库	<p>包括 Windows 帮助 (.chm) 格式的以下所有文档，以便可以在所有文件中搜索。还包括指向 Acrobat (.pdf) 格式的指南的链接。</p> <p>可以通过以下多种方式访问此库：</p> <ul style="list-style-type: none"> ■ 在 Windows 资源管理器中，浏览至 Enterprise Vault 安装文件夹的子文件夹 Documentation\language\Administration Guides，然后打开 EV_Help.chm 文件。 ■ 在管理控制台的“帮助”菜单中，单击“Enterprise Vault 的帮助”。
介绍和规划	提供 Enterprise Vault 功能的概述。
<i>Deployment Scanner</i>	介绍在安装 Enterprise Vault 之前如何检查必备软件和设置。
安装和配置	提供关于设置 Enterprise Vault 的详细信息。
升级说明	描述如何将现有 Enterprise Vault 安装升级到最新版本。
设置 Domino 服务器归档	介绍从 Domino 邮件文件和日记数据库归档项目的方式。
设置 Exchange Server 归档	介绍从 Microsoft Exchange 用户邮箱、日记邮箱和公用文件夹中归档项目的方式。
设置文件系统归档	介绍归档在网络文件服务器上保存的文件的方式。
设置 IMAP	描述如何配置 IMAP 客户端对 Exchange 归档和 Internet 邮件归档的访问权限。
设置 SharePoint 服务器归档	介绍如何从 Microsoft SharePoint Server 归档文档。
设置 Skype for Business 归档	介绍如何归档 Skype for Business 会话。
设置 SMTP 归档	介绍从其他邮件服务器归档 SMTP 邮件的方式。
使用 Microsoft 文件分类基础架构进行分类	介绍如何使用内置于 Windows Server 最新版本中的分类引擎对所有新的和现有的归档内容进行分类。
使用 Veritas Information Classifier 进行分类	介绍如何使用 Veritas 信息分类器根据一套全面的行业标准分类策略来评估所有新的和归档的内容。如果您不熟悉 Enterprise Vault 分类，建议使用 Veritas 信息分类器，而不使用缺乏直观性的旧版文件分类基础架构引擎。
管理指南	介绍执行每日管理过程的方式。

文档	注释
PowerShell Cmdlet	介绍如何通过运行 Enterprise Vault PowerShell cmdlet 执行各种管理任务。
审核	介绍如何收集有关 Enterprise Vault 服务器上的事件的审核信息。
备份和恢复	介绍如何实施有效的备份策略以防止数据丢失，以及如何提供在系统崩溃时进行恢复的方法。
报告	描述如何实施 Enterprise Vault Reporting，将提供关于 Enterprise Vault 服务器状态、归档和已归档项目的报告。如果您配置 FSA 报告，文件服务器及其卷可以获得其他报告。
NSF 迁移	介绍如何将 Domino 和 Notes NSF 文件内容导入到 Enterprise Vault 归档。
PST 迁移	介绍如何将 Outlook PST 文件内容迁移到 Enterprise Vault 归档。
实用程序	介绍了 Enterprise Vault 工具和实用程序。
注册表值	一个参考文档，列出了可用于修改 Enterprise Vault 行为的许多方面的注册表值。
管理控制台帮助	Enterprise Vault 管理控制台的联机帮助。
Enterprise Vault Operations Manager 帮助	Enterprise Vault Operations Manager 的联机帮助。

有关受支持设备和软件版本的最新信息，请参见 Enterprise Vault [Compatibility Charts](#)。

Enterprise Vault 培训模块

Veritas 教育服务提供 Enterprise Vault 的全面培训，从基本管理到高级主题和故障排除。有多种培训形式可供选择，包括基于课堂的培训和虚拟培训。

有关 Enterprise Vault 培训、课程路径和认证选项的详细信息，请参见 <https://www.veritas.com/services/education-services>。

Enterprise Vault 审核简介

本章节包括下列主题：

- [关于 Enterprise Vault 审核功能](#)

关于 Enterprise Vault 审核功能

Enterprise Vault 包括可以为各个 Enterprise Vault 服务器启用的灵活审核。审核数据写入 SQL Server 数据库中，可以对一个站点中的所有 Enterprise Vault 服务器使用一个审核数据库。

Enterprise Vault 审核将记录以下内容：

- 事件发生的时间
- 启动活动的帐户
- 项目归档到的归档
- 事件的类别，例如查看、归档或删除

可以为多个不同类型的事件启用审核，例如可显示以下详细信息：

- 使用管理控制台执行的操作
- 搜索
- 查看项目
- 删除

对于大多数事件类型，可以指定摘要或详细信息的详细级别，或者同时指定两者：

- 摘要提供有关事件的信息，例如日期和时间、使用的帐户和使用的保管库。
- 详细信息则列出更多信息，例如从邮件中提取的内容（如主题、邮箱所有者和文件夹）。

您可以使用 SQL 查询查看审核数据库条目，或者使用审核查看器实用程序。

Enterprise Vault 提供 PowerShell cmdlet 用于管理 Enterprise Vault SQL 数据库。
有关详细信息，请参见“PowerShell Cmdlet”指南。

请注意，在启用审核时性能稍有下降。

默认情况下已禁用审核功能。

设置审核

本章节包括下列主题：

- [设置审核](#)
- [创建审核数据库](#)
- [配置审核类别](#)
- [启动或停止审核](#)
- [调整审核](#)
- [移动审核数据库](#)

设置审核

表 3-1 汇总了在设置审核功能时需执行的任务，并提供了指向其中包含详细信息的各个部分的链接。

表 3-1 用于设置审核功能的步骤

步骤	任务	详细信息
步骤 1	创建审核数据库。	为站点中的所有 Enterprise Vault 服务器创建一个审核数据库。 请参见第 11 页的 “创建审核数据库” 。
步骤 2	选择要审核的类别。	在站点中的每个 Enterprise Vault 服务器上配置审核类别。 请参见第 12 页的 “配置审核类别” 。

步骤	任务	详细信息
步骤 3	启动或停止审核。	需要在站点中的每个 Enterprise Vault 服务器上启动或停止审核。 请参见第 14 页的 “启动或停止审核” 。
步骤 4	如有必要，请调整审核。	可以通过更改 Enterprise Vault 服务可向审核数据库建立的连接数量，来调整审核。 请参见第 15 页的 “调整审核” 。

存在与 Enterprise Vault 审核的配置相关联的注册表设置。如果使用 Regedit 直接更改这些注册表设置，而不是使用 Enterprise Vault 管理控制台，则 Enterprise Vault 审核无法捕获有关做出更改的用户的信息。如果要记录此信息，请在以下注册表项下为这些设置配置 Windows 注册表项审核：

HKKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KVS\Enterprise Vault\Admin\Auditing。

注意： 始终使用 Enterprise Vault 管理控制台配置 Enterprise Vault 审核。不要直接更改关联的注册表值。

创建审核数据库

本部分介绍如何使用管理控制台来创建审核数据库。

必须向审核数据库应用适当的安全性。应该考虑仅允许特权用户（如 Vault Service 帐户）访问数据库。例如，您可能希望阻止 Vault Service 帐户删除或修改审核数据库中的归档权限记录。

Enterprise Vault 数据库包含可用于增强您环境中的数据库安全性的角色。有关如何使用数据库角色来提高审核数据库的安全性的信息，请参见[Using sing SQL Database Roles in Enterprise Vault, Compliance Accelerator, and Discovery Accelerator](#)（在 Enterprise Vault, Compliance Accelerator 和 Discovery Accelerator 中使用单个 SQL 数据库角色）。

注意： 审核数据库可能会增长到很大，并且有时可能需要执行到新数据库的翻转，或者需要从数据库中删除一些条目来回收一些磁盘空间。有关详细信息，请参见 Enterprise Vault [SQL Best Practices](#)（SQL 最佳做法）指南。

创建审核数据库

- 1 在管理控制台的左侧窗格中，右键单击 Enterprise Vault 目录，然后在上下文菜单中单击“启用审核”。
- 2 在“审核数据库位置”下，单击“浏览”以显示审核数据库的可用位置。
- 3 如果希望为审核数据库创建新的文件夹，请单击“新建文件夹”。
- 4 单击要用于审核数据库的位置，然后单击“确定”。
- 5 在“事务日志位置”下，单击“浏览”以显示审核数据库事务日志的可用位置。
- 6 如果希望为事务日志创建新的文件夹，请单击“新建文件夹”。
- 7 单击要用于日志的位置，然后单击“确定”。
- 8 单击“确定”关闭“配置审核”对话框。
- 9 请等待几分钟，以便 Enterprise Vault 创建数据库。
- 10 当 Enterprise Vault 显示确认消息，告知您它已创建了审核数据库时，请单击“确定”关闭该消息框。

将在与 Enterprise Vault 目录数据库所在的同一 SQL Server 上创建审核数据库。但是，如果需要，您也可以将审核数据库移到其他服务器上。

请参见第 15 页的[“移动审核数据库”](#)。

配置审核类别

审核类别将确定审核功能可收集的不同信息类型。创建审核数据库后，可以使用 Enterprise Vault 管理控制台选择审核类别。所有类别都可以记录摘要审核数据，并且有些类别还可以记录详细数据。

审核类别将应用于您在管理控制台的“Enterprise Vault 服务器”容器中选择的企业 Vault 服务器。如果存在多个 Enterprise Vault 服务器，则需要依次选择每个服务器，并为每个服务器配置审核类别。建议在与 Enterprise Vault 目录关联的站点中的所有 Enterprise Vault 服务器上一致地设置审核类别。否则，将导致您环境中的审核数据不一致。如果选择类别“归档权限”，则务必在所有 Enterprise Vault 服务器上均选择此类别。

在 Enterprise Vault 管理员更改审核配置时，事件 ID 4288 会报告审核功能是正在运行（已启用）还是已停止（已禁用）、每个审核类别的状态以及执行了更改的管理员的身份。此外，还会创建一个具有相同信息的审核数据库条目。

您可以在审核功能运行或停止时修改审核类别。

表 3-2 审核类别

类别	说明
管理活动	在 Enterprise Vault 管理控制台或 Management Shell 中所做的配置更改，如添加新的任务、创建归档或启用邮箱。
高级搜索	执行的搜索，包括所用的词语和找到的项目数。
归档	手动归档或按计划归档的项目。
归档文件夹更新	要移至其他邮箱文件夹的已归档项目。
归档权限	<p>手动更改归档的用户或组访问权限。使用“归档属性”对话框或 Enterprise Vault 策略管理器 (EVP) 实用程序，可在 Enterprise Vault 管理控制台中的归档上设置手动权限。如果选择此类别，则应在站点中的所有 Enterprise Vault 服务器上选择该类别。</p> <p>请注意，此审核类别不会捕获对归档的自动访问权限的更改。自动归档权限是在原始内容源上设置的权限，并且会同步到 Enterprise Vault 归档。要捕获此信息，您必须在内容源应用程序中启用和配置审核。例如，用户对 Exchange Server 邮箱所做的访问权限更改会自动同步到关联的 Enterprise Vault 归档。要捕获这些权限更改，您必须在托管该邮箱的 Exchange Server 上启用和配置 Exchange Server 审核。</p>
分类	已归档项目的分类。
删除	出于以下原因而删除的已归档项目：保留期限已过期，因此用户已选择删除这些项目，或者第三方应用程序已请求删除这些项目以遵从数据保护法规。
Domino 归档	任何 Domino 归档活动。
Domino 还原	任何 Domino 还原活动。
Exchange 同步	记录 Exchange 托管内容设置的创建、修改和删除的详细信息。当被配置为从 Exchange 托管文件夹归档并与其托管内容设置同步时，Enterprise Vault 将记录有关详细信息。
FS 归档	文件系统归档活动。
GetOnlineXML	SharePoint Portal Server 中的文档检索。
索引操作	用于管理索引卷的索引子任务的启动和停止时间。还记录子任务在处理索引时遇到的任何严重错误。通过“管理索引”向导，可以管理索引卷。
移动归档	各个移动归档操作的详细信息。
NSF 迁移	从 NSF 文件中迁移的项目。

类别	说明
PST 迁移	从 PST 文件中迁移的项目。
还原	被还原的已归档项目。
保留类别更新	更改为已归档项目的保留类别。
SPS 归档	SharePoint 归档活动。
Saveset 状态	(用于支持。) 极少使用。记录 saveset 文件是否可用。
子任务控制	创建和修改子任务，例如控制移动归档操作的子任务。
取消删除	使用归档属性的“删除的项”选项卡上的选项“恢复项目”恢复的已删除项目。还会记录使用 FSAUndelete 实用程序恢复的快捷方式。
用户	您自己的审核条目。
查看	以 HTML 格式或原始格式查看已归档项目。
查看附件	查看 SharePoint Portal Server 中已归档项目。

配置审核类别

- 1 在管理控制台中，展开左侧窗格中的树，直到显示“Enterprise Vault 服务器”容器为止。
- 2 展开“Enterprise Vault 服务器”容器。
- 3 右键单击要配置审核的计算机，然后在上下文菜单中单击“属性”。
- 4 单击“审核”选项卡。
- 5 选中或清除审核类别。

表 3-2

- 6 单击“确定”保存所做的更改。

启动或停止审核

要启动或停止审核，您需要对每个 Enterprise Vault 服务器执行以下过程。

当审核启动或停止时，事件 ID 42388 会报告审核功能是正在运行（已启用）还是已停止（已禁用）、每个审核类别的状态以及执行了更改的管理员的身份。当 Enterprise Vault 管理服务启动时，如果审核功能正在运行，会报告事件 ID 4286，如果审核功能已停止，则报告事件 ID 4287。此外，还会创建一个具有相同信息的审核数据库条目。

启动或停止审核

- 1 在管理控制台中，展开左侧窗格中的树，直到显示 “Enterprise Vault 服务器” 容器为止。
- 2 展开 “Enterprise Vault 服务器” 容器。
- 3 右键单击要启动或停止审核的计算机，然后在上下文菜单中单击 “属性”。
- 4 单击 “审核” 选项卡。
- 5 要在 Enterprise Vault 服务器上启动审核，请选择 “根据以下类别审核条目”。
要在服务器上停止审核，请清除此设置。
- 6 单击 “确定” 保存所做的更改。

调整审核

每台启用了审核的计算机都只能与审核数据库进行有限数量的连接。会根据需要重用这些连接。审核将使用与审核数据库之间的连接池。可以让 Enterprise Vault 审核记录这些连接的使用率水平，然后，如有必要的话，可以按需要修改连接的数量。

调整审核

- 1 在管理控制台中，展开左侧窗格中的树，直到显示 “Enterprise Vault 服务器” 容器为止。
- 2 展开 “Enterprise Vault 服务器” 容器。
- 3 右键单击要为其启用或禁用连接信息记录功能的计算机，然后在上下文菜单中单击 “属性”。
- 4 单击 “审核” 选项卡。
- 5 单击 “高级”。
- 6 选中或清除 “日志数据库信息” 以打开或关闭日志记录功能。
- 7 如有必要，修改每个 Enterprise Vault Service 的连接数。
- 8 单击 “确定”。
- 9 在计算机上重新启动 Enterprise Vault 管理服务。

移动审核数据库

如果需要（例如在灾难恢复期间），可以将审核数据库移动到其他 SQL Server。移动数据库后，请在已启用审核的每台 Enterprise Vault 服务器上完成以下步骤。

移动审核数据库

- 1 将审核数据库移动到新的 SQL Server。
- 2 在 Enterprise Vault 服务器上，使用 ODBC 数据源管理器在 EVAudit ODBC 数据源上选择新的 SQL Server。
- 3 在 ODBC 数据源管理器为您提供机会时对数据源进行测试。

查看审核数据库条目

本章节包括下列主题：

- [关于查看审核数据库条目](#)
- [使用审核查看器查看审核数据库条目](#)
- [使用 SQL 查询查看审核数据库条目](#)

关于查看审核数据库条目

您可以使用 SQL 查询来查看和过滤审核数据库条目。您还可以使用脚本化功能自定义处理和显示条目的方式。

或者，Enterprise Vault 提供了审核查看器实用程序，可使用该实用程序查看和过滤审核条目。

使用审核查看器查看审核数据库条目

审核查看器允许您查看和过滤在 Enterprise Vault 审核数据库中记录的数据。可以指定要查看的数据、对数据进行排序以及将其复制到 Windows 剪贴板上。

使用审核查看器运行审核数据报告

按照此部分中的说明打开审核查看器，并生成关于审核数据库中数据的报告。

注意：如果计算机启用了用户帐户控制 (UAC)，则必须以管理员权限运行此实用程序。

使用审核查看器运行审核数据报告

- 1 在 Windows 资源管理器中，浏览到 Enterprise Vault 程序文件夹（例如，C:\Program Files (x86)\Enterprise Vault）。
- 2 双击 AuditViewer.exe。
- 3 在审核查看器窗口中，键入或选择要查看的记录的搜索条件。
下表提供了关于每个搜索词的信息。

用户名	采用 <i>domain\username</i> 的形式指定必需用户。
归档	指定所需归档的名称。您可以使用 Enterprise Vault 管理控制台来确定名称。
类别	从列表中选择要搜索的审核条目的类别。审核查看器只列出已捕获数据中存在的那些类别。
子类别	选择类别之后，从列表选择一个子类别。 <div><div>■ Item（项目） 将返回类别的摘要信息。</div><div>■ 如果选择 Detailed 作为类别，则 Information 记录中会包含更多信息。</div><div>■ All 将返回所选类别的摘要记录和详细记录。</div></div>
其实日期、结束日期	定义搜索审核记录的日期范围和时间范围。
信息包含	键入要在审核记录中搜索的关键词。
状态	从列表中选择要查看的记录的状态。
服务器	选择成为此搜索目标的 Enterprise Vault 服务器。
审核 ID	键入表示要查看的审核记录的一系列号码。
排序依据	选择对结果进行排序所依据的属性，并且选择希望审核查看器按照升序还是按照降序列出结果。
最多结果	选择是查看搜索找到的所有结果，还是只查看一部分结果。

- 4 单击“搜索”可生成报告。

从审核查看器中复制搜索结果

审核查看器在 **Search Results** 窗口中显示与搜索条件匹配的记录。

单击列标题可根据该列中的条目对这些记录进行排序。

可以将此窗口的内容复制到另一个应用程序中，如电子表格应用程序。

从审核查看器中复制搜索结果

- 1 在 **Search Results** 窗口中，突出显示要复制的记录。
- 2 右键单击这些记录，然后单击 **Copy**。
还可以按 **Ctrl+A** 和 **Ctrl+C** 将所有搜索结果复制到剪贴板中。
- 3 将记录粘贴到目标文档中。

更改审核查看器设置

可以更改要搜索的审核数据库。审核查看器还提供在 **Search Results** 窗口中隐藏或显示选定字段的选项。

更改审核查看器设置

- 1 在审核查看器主窗口中，单击 **Settings**。
- 2 在 **Settings** 窗口中，更改要搜索的审核数据库。还可以选择或清除要显示或隐藏的返回字段。

使用 SQL 查询查看审核数据库条目

我们建议您查询审核数据库中的数据库视图 **EVAuditView**。SQL 查询可以根据条件（例如，日期范围、用户名或 **ObjectID**）过滤审核条目。有关审核数据库条目的格式说明和不同类型的审核条目的 **EVAuditView** 列中值的解释，请参见本文档的附录。

请参见第 27 页的[“审核数据库条目的格式”](#)。

以下过程介绍如何使用 **SQL Server Management Studio** 进入并运行 SQL 查询。后面的部分将提供 SQL 查询示例，阐述该查询如何搜索数据库条目以执行项目删除操作。您可能需要出于显示数据保护法规遵从性等目的运行此类查询，以获得项目删除的证据。

请参见第 22 页的[“审核常规删除操作”](#)。

对归档访问权限的更改将显示为安全描述符定义语言 (SDDL) 字符串。**Enterprise Vault** 中随附了一个脚本，用于将这些字符串转换为一组更加用户友好格式的权限命令。

请参见第 20 页的[“以用户友好格式检索归档权限的审核更改”](#)。

使用 SQL Server Management Studio 查看审核数据库条目

- 1 启动 SQL Server Management Studio。
- 2 在标准工具栏上，单击“新建查询”。
- 3 在 SQL 编辑器工具栏上，从可用数据库的列表中选择 **EnterpriseVaultAudit**。
- 4 键入 SQL 查询以检索所需的审核条目。

此简单示例查询将按日期顺序从数据库视图 **EVAuditView** 中检索审核条目：

```
SELECT * FROM EVAuditView ORDER BY AuditDate DESC
```

以下是另一个示例查询。此示例查询根据日期范围和用户名过滤条目。

```
USE EnterpriseVaultAudit

DECLARE @StartDateTime datetime
DECLARE @EndDateTime datetime

SET @StartDateTime = '2017-10-05 08:00:00'
SET @EndDateTime = '2017-10-06 08:00:00'

SELECT * FROM [EnterpriseVaultAudit].[dbo].[EVAuditView]
WHERE AuditDate BETWEEN @StartDateTime and @EndDateTime
AND UserName in ('Org\HSmith', 'Org\JDoe')
ORDER BY AuditID
```

- 5 在 SQL 编辑器工具栏上单击“执行”，或按 F5 运行命令。

以用户友好格式检索归档权限的审核更改

通过使用“归档”属性中的“权限”选项卡或 Enterprise Vault 策略管理器 (EVP) 实用程序，管理员可以更改对归档的手动权限。在审核数据库条目中，对于 Windows 权限，对手动归档访问权限执行的更改以安全描述符定义语言 (SDDL) 字符串形式显示；对于 Domino 权限，对手动归档访问权限执行的更改以 XML 形式显示。

Enterprise Vault 中包含一个示例 PowerShell 脚本

ExampleEvPermissionsAuditHelper.ps1，用于说明您可以如何将这些字符串转换为更加用户友好格式的权限命令。此脚本输出中包含以下信息：

- 归档的标识详细信息。
- 已更改了权限的 Enterprise Vault 管理员的名称。
- 已为其在归档上设置了手动权限的每个管理员的新旧权限列表。

此示例脚本位于文件夹 `Enterprise Vault_installation\Auditing` 中。可以在审核数据库上运行此脚本，或修改此脚本以用于审核数据库处理过程中。Enterprise Vault Management Shell 不需要运行此脚本。

此示例脚本中的注释解释了此脚本的工作内容、运行此脚本所需的权限以及此示例脚本的局限性。您需要根据自己的环境相应更改此脚本中的值。

“归档”属性对话框和 EVPM 中可用的权限包括读取、写入和删除。这些权限与审核数据库条目中的更多粒度权限相等同。表 4-1 显示对管理员可用的权限与审核数据库条目（由示例脚本输出）中显示的基础权限之间的映射。

表 4-1 可用权限与脚本输出的权限的映射

“归档”属性和 EVPM 中的权限	示例脚本输出的权限
读取	READ_FOLDER READ_ITEM
写入	ADD_FOLDER ADD_ITEM CONTROL_FOLDER
删除	DELETE_FOLDER DELETE_ITEM

审核数据保护合规性

本章节包括下列主题：

- [审核常规删除操作](#)
- [审核特权删除操作](#)

审核常规删除操作

有些数据保护法规（例如，《欧盟通用数据保护条例》(GDPR)）涉及“被遗忘权”。此法规支持请求删除组织存储系统中无需再保存的个人信息。您可以使用 Enterprise Vault 审核提供已删除信息的相关证明。

本部分介绍如何设置 Enterprise Vault 以支持请求删除 Enterprise Vault 中的特定信息。示例搜索显示如何检索提供项目删除操作证据的审核条目。本部分中的示例与 Enterprise Vault 中的常规删除操作相关。

Discovery Accelerator 中提供了特权删除功能。此功能允许具有特殊权限的管理员删除项目以遵循数据法规。采用 Enterprise Vault API 的第三方应用程序也可以使用类似功能。这些操作的 Enterprise Vault 审核条目将标识删除操作已作为数据法规合规性的一部分执行。出于此原因，特权删除操作的 SQL 搜索和结果与常规删除操作的 SQL 搜索和结果略有不同。

请参见第 25 页的[“审核特权删除操作”](#)。

[表 5-1](#)举例说明了您可以采取哪些步骤将审核数据库条目提供为证据，证明已从归档中删除特定的数据。

为了便于搜索，此示例使用了 Enterprise Vault 分类功能。您可以配置 Enterprise Vault 分类功能，使其在归档时标记不同类型的信息。例如，Enterprise Vault 分类可将标记 `evtag.category:PII` 应用于个人身份信息 (PII)。

表 5-1 提供项目删除证据的相关步骤

步骤	操作	详细信息
1	检查是否未选择站点设置“启用恢复用户删除的项目”。	如果可能有“被遗忘权”请求，则不启用此站点设置十分重要。这可确保在执行“被遗忘权”请求后无法还原该项目。
2	检查是否已启用审核并选中所需的审核类别。	启用 Enterprise Vault 审核。 在 Enterprise Vault 服务器的属性中，需要为此示例启用的审核类别为“高级搜索”和“删除”。对于“删除”类别，摘要级别便已足够。
3	搜索要删除的项目。	在此示例中，我们使用 Enterprise Vault 搜索来搜索 Exchange 邮箱归档中要删除的数据。 执行搜索之前，请确保执行搜索的管理员对用户归档具有足够的权限，能够删除项目。 输入的搜索为：`evtag.category:PII` Enterprise Vault 搜索执行的实际搜索为： `'(NOT sens:2) AND (evtag.category:PII) '` 这意味着该搜索不会返回 Outlook 中标记为“私有”的任何项目；Enterprise Vault 搜索会自动执行此过滤。
4	使用 Enterprise Vault 搜索以删除所有返回的结果。	在搜索策略中，确保已启用项目删除。 在 Enterprise Vault 搜索中，右键单击要删除的项目并选择“删除”。
5	使用 Enterprise Vault 搜索重复相同的搜索。	重复相同的搜索以显示已删除正确的项目，这一点十分重要。
6	在审核数据库中，搜索删除操作条目。	使用合适的 SQL 查询提取审核跟踪的相关部分。搜索查询可基于审核日期、归档 ID 等。 请参见第 23 页的“常规项目删除审核条目的查询搜索示例”。 请参见第 26 页的“查询搜索特权删除审核条目示例”。

常规项目删除审核条目的查询搜索示例

以下简单查询将从审核数据库中检索指定时间段内的所有搜索和删除条目。

```
USE EnterpriseVaultAudit
SELECT * FROM [EnterpriseVaultAudit].[dbo].[EVAuditView]
```

```
WHERE CategoryName in ('Search', 'Delete')
AND AuditDate BETWEEN '2017-10-05 08:27:48' and '2017-10-05 08:32:37'
ORDER BY AuditID desc
```

以下 SQL 查询还可扩展此简单查询，对归档进行过滤。归档信息存储在 Enterprise Vault 目录中。

```
DECLARE @ArchiveId varchar(112)
DECLARE @StartDateTime datetime
DECLARE @EndDateTime datetime

SET @ArchiveId =
'1B29F35DAA512AC47A64558FDF7A614571110000example.local'
SET @StartDateTime = '2017-10-05 08:27:48'
SET @EndDateTime = '2017-10-05 08:28:37'

CREATE TABLE #ArchiveFolders
(
    VaultEntryId varchar(112)
)

INSERT INTO #ArchiveFolders
SELECT VaultEntryId
FROM [EnterpriseVaultDirectory].[dbo].[ArchiveFolderView]
WHERE ArchiveVEID = @ArchiveId

SELECT * FROM [EnterpriseVaultAudit].[dbo].[EVAuditView]
auditView LEFT JOIN #ArchiveFolders archFolder
ON archFolder.VaultEntryId = auditView.Vault
WHERE AuditDate BETWEEN @StartDateTime and @EndDateTime
AND CategoryName in ('Search', 'Delete')
ORDER BY AuditID

DROP TABLE #ArchiveFolders
```

表 5-2 显示由审核数据库的 SQL 查询返回的示例数据。列标题与审核数据库中的数据库视图 EVAuditView 相关。“示例值 (搜索)”列中的值显示了初始搜索为要删除的项目创建的审核条目。“示例值 (删除)”列中的值显示了用户 jdoe 删除项目时创建的审核条目。

对于表 5-1 中的步骤，最终搜索还会列出审核条目，显示该项目不再存在。表 5-2 中不包括此审核条目。

有关审核数据库条目的格式说明和不同类型的审核条目的 EVAuditView 列中值的解释，请参见本文档的附录。

表 5-2 SQL 查询返回的示例审核条目值

EVAuditView 列标题	示例值（搜索）	示例值（删除）
AuditID	3582	3584
Status	SUCCESS	SUCCESS
AuditDate	31/08/2017 10:03:37	31/08/2017 10:03:44
UserName	example\jdoe 执行搜索操作的用户。	example\jdoe 执行删除操作的用户。
CategoryName	Search	Delete
SubCategoryName	Searches	Item
ObjectID (Saveset and/or Folder ID)		#142\$1610D28B10DB21647B11EEF479019B70B1110000example.local
Vault (Archive or Folder ID)	16454F118169EDE48822DC10CE69307CA1110000example.local	1610D28B10DB21647B11EEF479019B70B1110000example.local
Info	Query '(NOT sens:2) AND (evtag.category:PII)', matching '8' entries, viewing range '1' to '100'	
MachineName	EVServer1	EVServer1

审核特权删除操作

通过将法规审阅者角色分配给选定的 Discovery Accelerator 客户端用户，您现在可以允许他们从 Enterprise Vault 归档中永久删除项目。通过与角色关联的特权删除权限，这些用户可以标记案例审阅集中的项目以从归档中删除。有关特权删除功能的详细信息，请参见 *Discovery Accelerator Administrator's Guide*（《Discovery Accelerator 管理指南》）。

采用 Enterprise Vault API 的第三方应用程序也可以使用遵从性删除功能。必须将运行第三方应用程序的用户分配给 Enterprise Vault 遵从性删除应用程序角色。

Enterprise Vault 审核会记录有关使用 Discovery Accelerator 中的特权删除执行的遵从性删除以及使用 Enterprise Vault API 的第三方应用程序中的遵从性删除的其他信息。

您可以在审核数据库上运行 SQL 查询，以检索有关遵从性删除操作的信息。

查询搜索特权删除审核条目示例

以下示例查询将搜索审核数据库中指定日期内的项目删除操作：

```
USE EnterpriseVaultAudit
GO
SELECT * FROM EVAuditView WHERE CategoryName = 'Delete' AND
SubCategoryName = 'Information' AND AuditDate BETWEEN
CONVERT(datetime,'mm-dd-yyyy',110) and
CONVERT(datetime,'mm-dd-yyyy',110)
```

表 5-3显示了此查询返回的审核条目示例值。

表 5-3 SQL 查询返回的示例审核条目值

EVAuditView 列标题	示例值（删除）
AuditID	4
Status	SUCCESS
AuditDate	2018-02-02 17:01:56.583
UserName	example\vsas 执行删除操作的用户。对于由 Discovery Accelerator 特权删除功能删除的项目， UserName 列将显示 Vault Service 帐户的名称。对由第三方应用程序删除的项目，将显示已分配给“遵从性删除应用程序”角色的用户。
CategoryName	Delete
SubCategoryName	Information
ObjectID	201802017502363~201802011626030000~Z~A158658C6FBE60B76 已删除项目的 saveset ID 。
Vault	600B5AA958C24411F9D0B892B91F5E4393B33DB7F88B8E551110000VS1 包含该项目的归档。
Info	<Delete ObjectType="Item" ObjectName="(null)"> <Property Name="EV_API_DELETION_LEVEL"> <Current Value="DELETION_LEVEL_COMPLIANCE"/> </Property> </Delete> 删除级别 DELETION_LEVEL_COMPLIANCE 表示已使用 Discovery Accelerator 中的特权删除或使用 Enterprise Vault API 的第三方应用程序中的遵从性删除删除了该项目。
MachineName	EVServer1

审核数据库条目的格式

本附录包括下列主题：

- [审核数据库条目的格式](#)

审核数据库条目的格式

在 Enterprise Vault 12.3 中，审核管理活动（“**管理活动**”审核目录）功能已得到增强。特别要指出的是，与以下领域中的管理活动相关的信息质量显著提升：

- Exchange、SMTP 和搜索策略
- Exchange 和 SMTP 任务
- Exchange 和 SMTP 目标
- Exchange 邮件类别
- 归档

还对基于角色的管理、保管库存储和分区管理以及高级设置的审核进行了改进。

改进的信息可用于使用管理控制台或 PowerShell Cmdlet 执行的活动。

注意：Veritas 正增强对多个版本的 Enterprise Vault 审核。本附录中的详细信息可能在未来版本中有所更改。

审核数据库中的 EVAuditView 数据库视图可用于显示审核条目，由以下列组成：

表 A-1 EVAuditView 列说明

列标题	内容的说明
AuditID	审核条目的唯一标识符。
Status	SUCCESS 或 FAILURE。操作是已成功完成还是失败。

列标题	内容的说明
AuditDate	生成审核条目的操作的日期和时间。
UserName	执行操作的用户。
CategoryName	审核类别，如 Enterprise Vault 服务器的“计算机属性”中所定义。
SubCategoryName	审核条目的更具体分类。
ObjectID	已更改的实体的 ID，例如 Saveset ID 、站点 ID、归档 ID。
Vault	仅对于大量审核，此列通常包含归档 ID 或 ArchivePoint ID 。
Info	自由格式文本提供有关所执行操作的更多信息。 在 Enterprise Vault 12.3 及更高版本中，有关审核操作的更多详细信息将在此列中提供。不同审核条目中此列的内容是本附录的主题。
MachineName	从中生成审核条目的计算机。

Info 列已引入一种新格式，能够以结构化和一致的方式显示审核操作的有关信息。本附录的其余部分介绍了各种审核条目中 Info 列的内容。请注意，完整审核条目还包含上述列出的信息，例如日期和时间、执行操作的用户，以及已更改的实体的 ID。

我们建议您使用 SQL 查询根据条件（例如日期范围、用户名或 ObjectID）查看和过滤审核条目。

要在结果中返回格式化的 XML，请使用类似如下的查询：

```
USE EnterpriseVaultAudit
SELECT TOP 50 ObjectID, AuditDate, UserName,
    TRY_CAST(info AS XML) AS infoXML
FROM EVAuditView
ORDER BY auditid DESC
```

简单审核条目中的信息内容

以下示例显示了在更改 **Exchange** 邮箱策略中的设置时所创建的审核条目中 Info 列的内容。表 A-2 介绍了包括的值。

```
<Update ObjectType="ExchangePolicyView"
    ObjectName="Exchange Mailbox Policy 2">
  <Property Name="ProcessUnreadMail">
    <Previous Value="0" />
    <Current Value="1" />
  </Property>
```

```
<Property Name="ProcessUnreadMail:TextValue">
  <Previous Value="Off" />
  <Current Value="On" />
</Property>
</Update>
```

表 A-2 示例中 XML 字段的说明

XML 字段	说明
Update	操作的类型。通常为 Create、Update 或 Delete。
ObjectType	操作影响的实体的类型。这通常是数据库表或已更改视图的名称。但是，在某些条目中会提供更易用的名称。
ObjectName	已更改的实体的名称。如果没有合适的值，则可能不会填充 ObjectName。
Property Name	与实体相关的属性的名称。（请参见注释 1。） 对于 Create 和 Delete 操作，列出了大多数属性，因为它们均获得或缺少一个值。（请参见注释 2。） 对于 Update 操作，仅包括已更改的属性。（请参见注释 3。） Property Name 字段末尾的 :TextValue 指示以下值是设置的文本值。在示例中，为值 "0" 和 "1" 显示的文本值为 "Off" 和 "On"。
Previous Value	执行操作之前属性的值。
Current Value	执行操作之后属性的值。

说明

- 1 名称通常是数据库中使用的名称，因此它可能不会与用户界面中的名称完全匹配。
- 2 为避免不必要的审核跟踪膨胀，部分非常频繁更改的属性不包括在内，例如 Exchange 邮箱的大小。
- 3 上下文中偶尔会包括其他属性。这也适用于其他类型的审核条目。

组合属性的信息内容

对于 Enterprise Vault 数据库中的某些设置，多个设置由单个值表示。审核条目将这些设置拆分为单独的属性。在 Update 条目中，通常只显示已更改的设置。

在 Exchange 邮箱策略的“快捷方式内容”选项卡上更改设置“包括横幅”和“包括归档项目的链接”之后，已在审核条目中生成以下示例 Info 内容。这两个设置作为单个值存储在 Enterprise Vault 数据库中。

```
<Update ObjectType="ExchangePolicyView"
  ObjectName="Exchange Mailbox Policy 2">
  <Property Name="excShortcutDetail">
    <Previous Value="1000005" />
    <Current Value="1000029" />
  </Property>
  <Property Name="excShortcutDetail:IncludeArchivedBanner">
    <Previous Value="False" />
    <Current Value="True" />
  </Property>
  <Property Name="excShortcutDetail:IncludeLinkToArchivedItem">
    <Previous Value="False" />
    <Current Value="True" />
  </Property>
</Update>
```

如您所见，“包括横幅”和“包括归档项目的链接”设置的有关信息将显示为单独属性。

多个设置存储在单个属性中时的信息内容

当删除 SMTP 目标时，已在审核条目中生成以下示例 Info 内容。

```
<Delete ObjectType="SmtptargetViewEx"
  ObjectName="JDoe@example.com">
  <Property Name="TargetId">
    <Current Value="19" />
  </Property>
  <Property Name="Address">
    <Current Value="JDoe@example.com" />
  </Property>
  <Property Name="poName">
    <Current Value="Default SMTP Policy" />
  </Property>
  <Property Name="RetentionCategoryName">
    <Current Value="RetCat01" />
  </Property>
  <Property Name="poPolicyEntryId">
    <Current Value="1781F4D98B1045F438445AC9
      8AD9579331s10000ev.local" />
  </Property>
  <Property Name="RetentionCategoryId">
    <Current Value="141E6B5A255237C4D83BB499
      390F27F091b10000ev.local" />
  </Property>
```

```
</Property>
<Property Name="ArchivingEnabled">
  <Current Value="1" />
</Property>
<Property Name="TargetType">
  <Current Value="1" />
</Property>
<Property Name="ArchiveInformation">
  <Current Value="<AI tn="JDoe@example.com" tid="19"
    an="Archive1" at="2049" aid="1868FD2720BFF62
    4483309845BDCCFEDB1110000ev.local" vs="Store1"
    ev="ev.local"/><AI tn="JDoe@example.com" tid=
    "19" an="Archive2" at="2049" aid="151D27
    0BA9638354DBE2B02FBFF7AF25C1110000ev.local" vs="Store1"
    ev="ev.local"/><AI tn="JDoe@example.com" tid="19"
    an="Archive3" at="2049" aid="13C3DC68A1FB836
    479CA542E4AE0CF9761110000ev.local" vs="Store2"
    ev="ev.local"/>" />
</Property>
</Delete>
```

ArchiveInformation 属性包含提供已分配给 SMTP 目标的三个归档的详细信息的 XML。

要使 ArchiveInformation 属性中的信息更具可读性，需为每个归档创建单独的审核条目。以下示例显示了上述 ArchiveInformation 属性中 Archive3 的审核条目。

```
<Delete ObjectType="SmtpTargetViewEx:ArchiveInformation"
ObjectName="JDoe@example.com">
  <Property Name="TargetAddress">
    <Current Value="JDoe@example.com" />
  </Property>
  <Property Name="TargetId">
    <Current Value="19" />
  </Property>
  <Property Name="ArchiveName">
    <Current Value="Archive3" />
  </Property>
  <Property Name="ArchiveType">
    <Current Value="2049" />
  </Property>
  <Property Name="ArchiveId">
    <Current Value="13C3DC68A1FB836479CA542
    E4AE0CF9761110000ev.local" />
```

```

</Property>
<Property Name="VaultStoreName">
  <Current Value="Store2" />
</Property>
<Property Name="EvServer">
  <Current Value="ev.local" />
</Property>
</Delete>

```

将单个审核条目拆分为多个条目有助于提高清晰度。例如，对于基于角色的管理更新和 SMTP 策略中的 X 标头管理，可能需要创建多个审核条目。